CLAIMS

Please amend the Claims as follows:

1. (Original)   A method for secure data transmission using multiple encryption keys comprising:

dividing a message object to be encrypted into a plurality of portions, each portion being associated with a shift point;

utilizing a first key to encode a first portion of the message object; when a first shift point occurs, generating a second key by executing a function that uses the first key and additional information; and

utilizing the second key to encode a second portion of the message object; upon completion of encoding of all of the plurality of portions of the message object, transmitting the encrypted message object to a receiver and destroying the keys.

2. (Original)   The method of claim 1, further comprising:

when each subsequent shift point occurs, generating a subsequent key by executing the function using a current key and additional information; and

utilizing the subsequent keys to encode subsequent portions of the message object.

3. (Original)   The method of claim 1, further comprising transmitting at least a portion of the additional information to the receiver for decoding of the encrypted message, wherein the portion of the additional information comprises a password and shift points.

4. (Original)   The method of claim 1, wherein the additional information comprises a password, an iteration value, and a symbol value, and the function executed is a hash algorithm.

5. (Original)   The method of claim 1, wherein the first key is a piece of digital media.

6. (New)   The method of claim 1, further comprising a step of: exchanging only the first key between a receiver and a sender.